

HARDWARE AUTHENTICATION SYSTEM AND METHOD

Field of the Invention

The present invention relates generally to component authentication and in particular to a hardware authentication system and method.

5

Background of the Invention

It is common practice in many industries to design equipment including modular hardware components. This allows hardware components to be replaced or exchanged with ease without requiring overall equipment modification. In many areas, equipment suppliers have found copying of their hardware components to be a problem. It has been found that unauthentic components sometimes do not meet the equipment suppliers' quality standards and/or do not interface properly with the equipment. Customers experiencing difficulty with unauthentic components often attribute the negative experiences to the equipment suppliers. This has led equipment manufacturers to incorporate authentication mechanisms into their equipment to inhibit unauthorized copies of hardware components from being used in their equipment.

For example, U.S. Patent No. 4,723,284 to Monk et al discloses a hardware authentication system for a public key communications network. The public key network includes at least one user terminal and at least one hardware authentication terminal coupled to the user terminal. The authentication terminal generates and stores a plain text message therein. The authentication terminal also generates from the plain text message, a cipher text message by transforming the plain text message with the public key of the user terminal and transmits the cipher text message to the user terminal. The user terminal is adapted to receive the cipher text message and transform the cipher text message with its private key to obtain a plain text message. The user terminal also transmits the plain text message back to the authentication terminal. The authentication terminal compares the plain text message received from the user terminal with the plain text message stored therein to determine coincidence. If the two plain text messages match, the authentication terminal generates an authentic user signal indicating that the user terminal is the hardware terminal associated with the public key.

A-1000-00000000000000000000000000000000

20

25

30

U.S. Patent No. 4,799,635 to Nakagawa discloses a system for determining the authenticity of computer software stored in a ROM cartridge when used with a main processor unit. To verify that the ROM cartridge is authentic, duplicate semiconductor devices are included in the ROM cartridge and the main processor unit. The semiconductor device associated with the ROM cartridge acts as a key device and the semiconductor device in the main processing unit acts as a lock device. The key and lock devices are synchronized and execute the same arithmetic operation according to pre-programming. The results of the executed arithmetic operations are exchanged between the semiconductor devices and compared. If the results agree, the ROM cartridge is determined to be authentic and the main processing unit is allowed to operate. If the ROM cartridge is determined to be unauthentic, the main processing unit is continuously reset inhibiting it from operating.

U.S. Patent No. 4,766,516 to Ozdemir et al discloses a security system and method for protecting an integrated circuit from unauthorized copying. During design the integrated circuit is provided with at least one additional circuit element that does not contribute towards the function of the integrated circuit. Rather, the additional circuit element is designed to inhibit operation of the integrated circuit when an unauthorized copy of the integrated circuit is made. The additional circuit element has the visible appearance of being functionally interconnected to the integrated circuit but actually is not. Thus, in an authentic device, the additional circuit element is isolated from the integrated circuit. However, when a copy is made, if the copier copies the integrated circuit according to its visual appearance, the additional circuit element will be physically connected to the integrated circuit and the operation of the additional circuit element will inhibit proper operation of the integrated circuit.

Although the above-identified references disclose systems and methods to deter copying, new authentication systems and methods are of course desired. It is therefore an object of the present invention to provide a novel hardware authentication system and method.

Summary of the Invention

According to one aspect of the present invention there is provided a hardware authentication system for equipment including at least one removable hardware component comprising:

5 a processing unit within said equipment and including a first pseudo-random number generator responsive to at least one non-deterministic event for generating a pseudo-random number; and

10 a second pseudo-random number generator on said removable hardware component, said second pseudo-random number generator also being responsive to said at least one non-deterministic event and generating a pseudo-random number, said processing unit comparing the pseudo-random numbers generated by said first and second pseudo-random number generators to detect coincidence and thereby determine authenticity of said hardware component.

15 In a preferred embodiment, the first and second pseudo-random number generators are responsive to non-deterministic and periodic events. Each of the pseudo-random number generators includes a counter that increments its count in response to non-deterministic events; a register that rotates its contents in response to periodic events; and logic coupling the counter and the register and modifying the register contents using the value of the counter prior to rotation of the contents of the register.

20 It is also preferred that the equipment is a private branch exchange and the removable component is a line card. In this case, the non-deterministic event is a busy state of a circuit of the line card resulting due to an off-hook condition of a telephone set connected to the circuit.

25 According to another aspect of the present invention there is provided a method of authenticating a removable hardware component installed in equipment, said method comprising the steps of:

30 providing a first pseudo-random number generator in said equipment that is responsive to at least one non-deterministic event for generating a pseudo-random number;

00000000000000000000000000000000

providing a second pseudo-random number generator on said hardware component that is also responsive to said at least one non-deterministic event for generating a pseudo-random number;

5 comparing the pseudo-random numbers generated by the first and second pseudo-random number generators at intervals to detect coincidence and thereby determine authenticity of said hardware component.

The present invention provides advantages in that unauthorized hardware components installed in equipment can be detected and inhibited from operating properly when used in the equipment. Since the first and second pseudo-random number generators generate pseudo-random numbers in response to variable events that occur within the equipment, the pseudo-random numbers generated by the pseudo-random number generators are difficult to predict making it extremely difficult for unauthentic hardware components to subvert the authentication system. Since authentic components are compatible with the equipment, quality standards and component compatibility can be ensured.

Brief Description of the Drawings

An embodiment of the present invention will now be described more fully with reference to the accompanying drawings in which:

20 Figure 1 is a schematic diagram of equipment incorporating a hardware authentication system in accordance with the present invention; and

Figure 2 is a schematic diagram of a pseudo-random number generator incorporated within a replaceable hardware component and forming part of the hardware authentication system of Figure 1.

Detailed Description of the Preferred Embodiment

The present invention relates to a hardware authentication system and method to determine the authenticity of a replaceable hardware component installed within equipment. In the preferred embodiment, the replaceable hardware component includes a pseudo-random number generator that is responsive to non-deterministic and periodic events and generates pseudo-random numbers. A processing unit in the equipment executes a software version of the same pseudo-random number generator

and compares the numbers it generates with the pseudo-random numbers generated by the pseudo-random number generator in the hardware component, at selected intervals. If the numbers match, the hardware component is considered to be authentic. If the numbers do not match, the hardware component is considered to be unauthentic and its operation within the equipment is inhibited. A preferred embodiment of the present invention will now be described with reference to Figures 1 and 2.

Turning now to Figure 1, equipment 10 including a replaceable hardware component 12 is shown. The hardware component 12 is releasably connected to the equipment 10 to facilitate replacement. The equipment 10 has a processing unit 14 executing an authentication program 15 including a software-based pseudo-random number generator 16. The replaceable hardware component 12 also includes a pseudo-random number generator 20. The authentication program 15 and the pseudo-random number generator 20 constitute a hardware authentication system designed to determine the authenticity of the hardware component 12 installed in the equipment 10.

As can be seen in Figure 2, the pseudo-random number generator 20 includes an 8-bit counter 22 having a plurality of parallel output pins Q_0 to Q_7 , a clock pin CLK and a reset pin R. The clock pin CLK receives input in response to the occurrence of a non-deterministic event. The output pins of the counter 22 are coupled to an array of XOR gates 28. The output pins of the XOR gates 28 lead to respective input pins D_0 to D_7 of an 8-bit register 30. The register 30 also includes a plurality of output pins Q_0 to Q_7 , a clock pin CLK and a reset pin R. The pseudo-random number generated by the pseudo-random number generator 20 is held by the register 30 and can be read via its output pins Q_0 to Q_7 . Each output pin of the register 30 is also coupled to an input pin of a respective XOR gate 28. The clock pin CLK receives input at periodic intervals.

Preferably, the counter 22, the register 30, the XOR gates 28 and the address decoding for the clock pins of the counter and register are contained within a single physical device, such as for example an ASIC or programmable logic device. In this way, generation of pseudo-random numbers by the pseudo-random number generator 20 cannot be easily observed or derived.

Similar to pseudo-random number generator 20, software pseudo-random number generator 16 includes a software counter, a software register and software logic for performing XOR operations on the software register contents using the count values output by the software counter. The pseudo-random number generator 20 is also responsive to the non-deterministic and periodic events.

In the preferred embodiment, the removable hardware component 12 is a twelve (12) circuit line card for a private branch exchange (PBX) 10. The non-deterministic event used to increment the counter 22 is any one of the line card circuits entering the busy state. This non-deterministic event occurs whenever a telephone set connected to a line card circuit enters an off-hook state.

The periodic input used to rotate the register is generated by the authentication program 15 every hour. The hardware component authentication process will now be described with particular reference to Figure 2.

Initially the counter 22 and register 30 as well as the software counter and register are reset by the authentication program 15. During normal operation, whenever a telephone set connected to one of the line card circuits enters an off-hook state, an input signal is applied to the clock pin CLK of the counter 22 causing the counter to increment its count value. The incremented count value output by the counter 22 is conveyed to the XOR gates 28, which also receive the register contents. The outputs of the XOR gates 28 are applied to the input pins D₀ to D₇ of the register 30 thereby to modify the register contents. Every hour, the authentication program 15 generates a signal that is applied to the clock pin CLK of register 30 causing the register to rotate the value therein by one bit position.

The software pseudo-random number generator 16 executed by the processing unit 14 is also responsive to the non-deterministic and periodic events and generates the same pseudo-random numbers.

Each hour after the register contents have been rotated, the authentication program 15 executed by the processing unit 14 reads the contents of the register 30 and the software register and compares the pseudo-random numbers. If the numbers match, the line card 12 is considered to be authentic and operation of the line card 12 within the PBX 10 continues. If however the numbers do not match,

the authentication program 15 generates a flag causing the processing unit 14 to inhibit further operation of the line card 12 within the PBX 10.

As will be appreciated, the hardware authentication system periodically checks the authenticity of replaceable hardware components within the equipment and inhibits an unauthentic hardware component from being used. Since the pseudo-random numbers generated by the software pseudo-random number generator and the hardware pseudo-random number generator are based on non-deterministic events, generation of the pseudo-random numbers cannot be easily observed or derived.

Although the pseudo-random number generator 20 shows all of the bits of the counter 22 and register 30 being XORed, the XORing operation can be performed only on selected bits if desired. Also, although the contents of the register 30 are described as being rotated by one bit on each periodic signal, the register contents can of course be rotated by more than one bit position on each periodic signal or not at all. Alternatively, more than one periodic signal may be required in order to rotate the register contents by one bit. In this case, additional logic is required to rotate the register contents every n^{th} periodic signal. Furthermore, if desired the counter 22 and/or register 30 can be preset with values at the time the pseudo-random number generator 20 in the hardware component 12 is initialized. The values can be preset or can be read from a variable source such as for example a real time clock. Also, if desired, the length of the counter 22 and register 30 can be increased or decreased. If the pseudo-random number generator 20 is modified in one or more of the above described manners, those of skill in the art will recognize that the software-based pseudo-random number generator 16 is of course modified in the same manner.

Although the hardware pseudo-random number generator is described as including a binary counter, a register and an array of XOR gates, the counter, register and XOR functions may be embodied in a microprocessor having appropriate firmware.

As will be appreciated, since authentic hardware components are compatible with the equipment, replaceable component integrity and quality standards can be maintained at the desired level.

Although a preferred embodiment of the present invention has been described, those of skill in the art will appreciate that variations and modifications may be made without departing from the spirit and scope thereof as defined by the appended claims.